Roundups

Air Force Research Laboratory AFRL

Unleashing the power of innovative aerospace technology....

news@*afrl*

Summer 1999 **Official voice of the Air Force Research Laboratory**

AFRL awards contracts for forensic software tools

by Francis L. Crumb, Information directorate

ROME, N.Y. — The Air Force Research Laboratory Information directorate awarded two contracts, with a combined value in excess of $250,000, to WetStone Technologies Inc. of Freeville, N.Y.

The first contract, "Synthesizing Information from Forensic Investigations,"or SiFi, is a two-year, $174,300 effort.

WetStone will design and build an open architecture that integrates future forensic methods and technologies. The architecture will isolate "forensic tools," or applications, from specific target hardware, from network effects and from operating system constraints.

"Most of the currently available computer forensic software tools are designed for use under very specific conditions," said John Feldman, program manager in the directorate's Defensive Information Warfare branch. "A generic, open architecture that can be applied across the board does not exist when investigators attempt to collect forensic information from and about computer systems.

"The way things are now, the available homogeneous forensics applications require the services of a highly trained computer expert to use and interpret. As a result, the evidence retrieved is poorly represented; that is to say, data requiring interpretation and integration is presented rather than information that is directly usable by investigators.

"The real payoff from this research will come during development of future forensic tools. This type of technology will give investigators the ability to 'plug-in' technologically advanced capabilities as they become available, without redesigning or recoding of the interfaces. The SiFi work will not only help us in the military with our specific needs, but will also be transitioned to the law enforcement computer forensics community."

The second AFRL contract with WetStone, "CSAP 21 Advancement and Expert Technology Exchange," is more than $88,200.

"WetStone will provide new technologies to assist computer network managers in monitoring their systems for unauthorized intrusions and threats," said Michael Nassif, program manger. "The new system will provide this capability with increased performance and affordability. It will also be compatible for civilian applications with commercial, off-the-shelf software."

Nassif said a prototype will be released for testing at several operational Air Force sites and has potential for use in a variety of government and commercial systems. **@**